CCR-25-70 Information Management: Automation Management Policy

Title: ***Information Management: Automation Management Policy***

Original Document Date: ***08/01/97***

Date: ***09/01/02***

Summary*:*

This is a change to Cadet Command Reg. 25-70, 3 February 1997. This change provides a new paragraph on Engineering Change Proposals - Software (ECP-S) for standardization and execution of Cadet Command Automated Data Processing Services.

POC/Impact:

Applicability. This regulation applies to all Cadet Command elements, to include Headquarters (HQ), Cadet Command, region HQ, Senior Reserve Officer's Training Corps (SROTC) battalions, Junior ROTC units, brigade commanders, Goldminer Teams, and forward-deployed activities.

Supplementation. This regulation may not be supplemented. Region specific guidance for the region HQ, SROTC battalions, JROTC units, Goldminer Teams, Forward-Deployed Commanders, and other command staff activities should be through a Memorandum of Instruction (MOI). Headquarters, Cadet Command staff offices are encouraged to publish internal standard operating procedures (SOPs) covering the management controls for their office.

Suggested Improvements. The proponent of this regulation is the Information Management Office, U.S. Army Cadet Command. Send comments and suggested improvements on **DA Form 2028** (Recommended Changes to Publications and Blank Forms) through channels to Commander, U.S. Army Cadet Command, ATTN: ATCC-RR, Fort Monroe, VA 23651-5000. Suggested improvements may also be submitted using **DA Form 1045** (Army Ideas for Excellence Program (AIEP) Proposal). Current CCR-25-70 supersedes CCR-25-70 dated 3 February 1997.

Please ensure that you have the following software loaded: Acrobat Reader 4.0 or >.

Details:

Table Of Contents

Chapter 1, Introduction

Chapter 2, Responsibilities

Chapter 3, Request for, and Approval of, Automation Services

Chapter 4, Computer Utilization

Chapter 5, Automated Information System (AIS) Accreditation

Chapter 6, Security

Chapter 7, Accountability

Chapter 8, Maintenance and Repair

Chapter 9, Training

Appendices

Chapter 1, Introduction TOC

1-1. Purpose. This regulation establishes Headquarters (HQ), Cadet Command's automation management policies. It addresses procurement,use, security, and maintenance of automation services (hardware/software/training). This regulation:

a. Defines the responsibilities of HQ, Cadet Command, region HQ, brigades, battalions, and extension centers for the use of automation services.

b. Provides procedures to assist the automation user in obtaining the most efficient and cost effective means to make and present sound decisions for mission accomplishment.

c. Clearly defines procedures for obtaining new and enhanced hardware and software and training.

d. Provides procedures to account for, repair, and maintain automation resources.

e. Provides procedures to maintain data and software integrity, and security of all automation resources.

1-2. References. Required and related publications are listed in **Appendix A**.

1-3. Explanation of Abbreviations and Terms. Abbreviations and special terms used in this regulation are explained in the glossary.

Chapter 2, Introduction TOC

2-1. Headquarters, Cadet Command.

a. The Headquarters, Cadet Command Information Management Office (IMO) has ultimate responsibility for all automation support for Cadet Command, region HQ, brigades, battalions, and extension centers. This support includes planning for procurement of hardware and software, security, training, financial support, and other automated services needed to accomplish the Cadet Command mission.

b. The HQ , Cadet Command IMO will--

(1) Develop Cadet Command Information Management's planning documents.

(2) In coordination with Resource Management, develop and execute the Command's Information Management Budget.

(3) Advise the Commander ad his/her staff on all information management matters.

(4) Provide user support for the HQ Commander and staff.

(5) Provide staff supervision to the region HQ Information Management Office.

(6) Serve as the automation point of contact for the integration of Cadet Command Systems with HQ, DOD; HQDA; and HQ, TRADOC automated systems.

(7) Recommend, approve, and disapprove requests for automation services and obtain TRADOC's formal approval when required.

(8) Acquire and manage the hardware, software, and training required for mission accomplishment.

(9) Supervise and manage contractor support required for Cadet Command automated systems.

(10) Design, assist in testing new and enhanced software, assist in the preparation of User Manuals, and field region, brigade, battalion, and extension center standard automatic data processing (ADP) systems.

2-2. Region, Headquarters. The Region Information Management Offices will--

a. Ensure that the ADP requirements, policies, and regulations for regions, brigades, battalions, and extension centers are compatible with HQ, Cadet Command's.

b. Ensure that brigade commanders, battalions, and extension centers comply with HQ, Cadet Command and region HQ policies, regulations, directives, and memorandums and letters of instruction for automation services.

c. Advise the region commander and his/her staff on all ADP matters.

d. Develop and submit the region's information management plan to HQ, Cadet Command.

e. Develop and execute the region's information management budget.

f. Provide ADP support to the region commander and his/her staff. This will include software development, testing, documenting, and maintaining region unique ADP systems.

g. When HQ, Cadet Command directs, design, develop, test, and document (User's Manual) those standard automated systems processed only at region HQ.

h. Develop the region's information management training program.

i. Review and approve and/or disapprove all **TRADOC Form 791-R** (Information Capability Requirements (CAPR) and **DA Form 5005-R**, Engineering Change Proposals - Software (ECP-S) submitted by region HQ staff, brigade commanders, battalions, and extension centers.

j. Prepare and submit Requirement Statements (RS) and ECP-Ss, along wit recommendations, to HQ, Cadet Command for action and provide status reports tot he initiator of those ECP-Ss.

k. Supervise the fielding of Cadet Command automated modules to battalions and extension centers and assist the battalions and extension centers in loading and operating the modules.

l. Notify HQ, Cadet Command, of all hardware and software problems which affect mission accomplishments.

2-3. Battalions and Extension Centers. The battalions and extension centers will--

a. Prepare and submit to region HQ **TRADOC Form 791-R** and **DA Form 5005-R**.

b. Operate, account for, and maintain all Cadet Command automation resources (personnel, hardware, software, and data) in accordance with HQ, Cadet Command and Region HQ policies, regulations, directives, memorandums, and letters of instruction for automation services.

c. Input and transmit accurate and timely data to Region HQ.

2-4. Functional Proponents.

a. The functional proponents--Personnel and Administration, Resource Management, Training, and Marketing, Operations, Public Affairs, High School, and Special Staff--are responsible for determining the automation needs for the Directorate and Special Staff.

b. The functional proponents will--

(1) Prepare ECPs for all new and enhanced software.

(2) Clearly define requirements in terms of data edits, formulas, computation required, and report formats.

(3) Clearly define processing dates, and dates for receipt of data.

(4) Test and approve all automated systems before the software is fielded. Tests are performed before the software is fielded. Tests are performed in-house and on-site when required. On-site testing will be held at the closest region, battalion, or extension center.

(5) With assistance from IMO staff, develop User Manuals and regulatory guidance. All guidance and instructions will combine manual and automated processes in "easy to use" format and language.

(6) Monitor data accuracy and timeliness.

(7) Attend and participate in the regular IMO ad DOIM In Process Reviews (IPRs) which impact the functional area of responsibility.

(8) Appoint Terminal Area Security Officers (TASO) who will ensure that all personnel requiring passwords have them, that passwords are not shared, and equipment is secured and operated properly.

(9) Ensure that all personnel receive office automation training through formal training or self-study.

(10) Ensure that new personnel are trained to use HQ, Cadet Command and region HQ unique application systems as they apply to their duty position.

Chapter 3, Request for, and Approval of, Automation Services TOC

3-1. Requests for Services.

a. Requests for, and approval of, hardware and software are accomplished through a series of planning documents; such as the Information management Modernization Plan and the RS.

b. Software required to meet special functional needs, and/or limited periods of time, will be evaluated on a case-by-case basis. Regardless of the requirement, maintenance, funding, personnel, and effect on the entire system will be considered.

3-2. Headquarters, Cadet Command. The Headquarters staff will submit requests for automation services to the Information Management Office.

3-3. Region Headquarters. Region HQ will submit annual updates to the 5-Year ADP Plan outlining automation services required for region HQ, brigades, battalions, and extension centers. These requirements will be submitted to **the Commander, U.S. Army Cadet Command, ATTN: IMO, Fort Monroe, Virginia 23651-5000**.

3-4. Battalions and Extension Centers. Battalions and extension centers will prepare **TRADOC Form 791-R**, **DA Form 5005-R**, and any region ADP request forms in accordance with region policies and instructions. Competed forms will be submitted to region HQ.

3-5. Acquisition and Funding of Computers for SROTC and JROTC

a. Purchase of automation equipment, computer upgrades, and software when approved by region HQ, must conform with the 5-year automation plan and have local available funds.

b. All computer purchases for Director of Army Instructions (DAI), SROTC, and JROTC units, to include computer upgrades and software acquisitions, require region HQ approval to assure

conformance with the Requirements Statement. Total purchase of upgrade or software may not $500 per computer. Servicing support installations will make final purchase determination based upon fund availability.

c. Maintenance/service support for computer equipment will be the responsibility of the servicing support installation based on availability of funds.

d. SROTC activities. Computer acquisition is authorized for senior units when approved by the region HQ. SROTC mission money (OMA) provided to support installations may only be used to purchase computer equipment or software, if the proposed purchase is in conformance with the 5-year automation modernization plan, and if it does not cause a funding shortfall.

e. JROTC activities.

(1) Region HQ have been funded for DAI computer acquisition. JROTC mission money (OMA) provided to support installations may be used to purchase DAI computer equipment or software only if the purchase is in compliance with the 5-year automation plan and does not cause a funding shortfall.

(2) Cadet Command has not been funded for the acquisition of computers for JROTC units. However, JROTC units may obtain computers using one of the methods prescribed in paragraph 3-6 below. Keep in mind that these methods have major cost advantages but may require additional time and work. For those who are "self starters," these are excellent ways to acquire equipment. Cadet Command did not receive additional funding to support computer upgrade/software purchases. Units must not use money needed to support their critical mission needs.

3-6. Obtaining SROTC and JROTC Automation Equipment at No Cost to Government

a. Identify automation needs to school officials and request purchase from school budget.

b. Lateral transfer of excess equipment from activity that is down sizing or that no longer requires computers/software. Property should be laterally transferred prior to being declared excess in the Defense Automation Resources Information Center (DARIC)/Automation Resources Management Systems (ARMS).

c. Obtain equipment that is declared excess through DARIC.

d. Utilize the Service Education Activity (SEA) Donation Program.

3-7. Processing Engineering Change Proposals - Sofware (ECP-S)

ECP-Ss are used to request new software development and to make changes to all cadet command automated modules/directories within the Cadet Command Information Management System (CCIMS) and stand alone systems.

a. All ECP-Ss are prepared on **DA Form 5005-R,** Engineering Change Proposal - Software (ECP-S). Please read paragraph 3-7 l. below for instructions on completing the **DA Form 5005-R.** there are two versions of **DA Form 5005-R** available for use: a manual form which can be obtained from the Information Management Office (IMO) and an automated form which can be found here --> **DA Form 5005-R**.

b. All ECP-Ss originating and/or prepared by HQ, Cadet Command functional users will be submitted to IMO. No ECP-Ss will be submitted directly to the programmers.

c. The Chief, ROTC Support Team-DOIM, will advise the IMO of there personnel resource requirements determined for each ECP-S and, based on established priorities for current committed effort, provide the best estimate of total effort that can be expended on completion of all outstanding ECP-Ss.

d. Based on this estimate, the IMO, in conjunction with the functional proponents, will stipulate which ECP-Ss are to be included in the next System Change Proposal (SCP) processing cycle. The functional user is also responsible for preparing user documentation within the same time frame allocated for the SCP cycle.

e. Requests for emergency ECP-Ss will be submitted verbally to the IMO with a hard copy ECP-S (**DA Form 5005-R**) follow-up within 5 working days. The verbal and hard copy request will include the exact change required and reason for the emergency. At no time will the functional user coordinate directly with the programmer. The IMO representative will coordinate with the Chief, ROTC Support Team, DOIM, immediately upon determining that an actual emergency exists.

f. Functional users will submit non-emergency ECP-S changes to the CCIMS modules/directories on **DA Form 5005-R** to the IMO. The ECP-S will be reviewed for clarity and validity, processed within 2 working days, and submitted to the Chief, ROTC Support Team-DOIM, for action. Those not in sufficient detail to determine programming requirements will be returned to the functional user for further clarification.

g. **Region Staff, Brigades, and Battalion Policy**. All ECP-Ss prepared by the region functional user, the brigades, and battalions will be submitted to the region IMO for evaluation and completion.

h. All ECP-Ss will prepared on **DA Form 5005-R** or special region forms. The regions will supply guidance and instructions for completion of special region forms.

i. The region IMOs will coordinate all ECP-Ss with the functional proponent of the specified module or project.

j. The region IMOs will forward all ECP-Ss affecting the CCIMS modules and other Cadet Command standard systems to: **Commander, U.S.Army Cadet Command, ATTN: IMO, Fort Monroe, Virginia 23651-5000**. A statement containing the region's recommendations will be included with these ECP-Ss.

k. All ECP-Ss for unique applications within the region will be processed by the region IMO.

l. Instructions for Preparation of **DA Form 5005-R**, Engineering Change Proposal - Software (ECP-S):

(1) The **DA Form 5005-R**, dated Nov 81, is a dual purpose form used to report problems or to propose changes pertaining to software baselines. Individuals preparing the form will mark appropriate box in the top right-hand block to indicate choice of problem report or ECP-S. The ECP-S is used to direct/recommend changes for region and HQ, Cadet Command systems. The

problem report is used to report problems for which the reporting person does not know the cause.

(2) Block 1. To: Enter mailing addresses as follows: **U.S. Army Cadet Command, Information Management Office, Fort Monroe, VA 23651-5000** or appropriate Region Information Management Office address.

(3) Block 2. From: Enter mailing address of originator. Include name of individual preparing form, if other than Point of Contact (POC) in Block 4.

(4) Block 3. Originator Number and Environment Code: Will be entered by HQ Cadet Command Information Management Office (IMO).

(5) Block 4. Point of Contact: Enter name and telephone number of individual who should be contacted to explain the reported problem or proposed change. Include alternate telephone numbers whenever possible. Use DSN number if available. A commercial number should include the area code.

(6) Block 5. Priority: For ECP-Ss, check appropriate block to indicate emergency, urgent, or routine. Emergency and urgent requests will be used when the work is required within a certain time, and it would have a significant impact on mission accomplishment.

(7) Block 6. Application C1 Baseline/Version: Leave blank. This block will be completed by HQ, Cadet Command or Region IMO.

(8) Block 7. Executive SW Baseline/Version: Leave blank. This block will be completed by HQ, Cadet Command or Region IMO.

(9) Block 8. Problem Date: For problem reports, enter date problems occurred (YYMMDD). If an ECP-S is being proposed, enter date ECP-S was prepared.

(10) Block 9. Job/Cycle/Program ID: Leave blank. Will be entered by HQ, Cadet Command, or Region IMO.

(11) Block 10. Title of Problem/Change: Enter a short descriptive title.

(12) Block 11. Description of Problem/Change: Describe the problem or proposed change in sufficient detail to permit ready identification and evaluation. Enter product (i.e., file ID, PCN, CSOM, End Users Manual, etc.) involved in the problem/change.

(13) Block 12. This block is to be completed by the originator. Affect on User: Describe adverse affects or improved characteristics the proposed change may have on the field user, to include the alternative of not making the proposed change.

(14) Block 13. Recommended Solution/Justification: The originator will enter a recommended solution and justification to support the proposed change. Include any action taken to resolve the problem.

(15) Block 14. Submitting Authority: This block must contain the date signed,name, and title, and signature of the individual with authority to approve origination of the ECP-S. This is

usually the functional proponent.

(16) Block 15. Remarks: This block is to be used by the originator to continue blocks 11 through 13 if needed. If necessary, Blocks 11 through 13 can be continued on separate sheets.

(17) Blocks 16 through 29. Leave blank. These blocks will be completed by HQ, Cadet Command or Region HQ.

Chapter 4, Computer Utilization

4-1. Headquarters, Cadet Command and Region HQ

a. Headquarters, Cadet Command and region HQ will follow the local installation's and headquarter's policies and procedures.

b. Regions may transmit and receive CCIMS data from HQ, Cadet Command, using the Non-Secure Internet Protocol Routing Network (NIPRNET) that is provided by the supporting military installation.

4-2. Battalions and Extension Centers

a. The Cadet Command computers installed at each battalion and extension center are to be used and accessed only for "Official Government Business."

b. The CCIMS software allows battalions and extension centers to:

(1) Enter data required by higher headquarters in the various automated Modules of the CCIMS--Branching, Cadet Database (Attritions, Commissionees, Enrollments, Scholarships, etc.), Cadet Pay, and Camps.

(2) Write queries and produce reports; such as the BLITZ, Mission Management Briefer, Cadet Record Brief, etc.

(3) Prepare, manage, and telecommunicate data files, word processing documents, spread sheets, and slides to region HQ and receive the same from region HQ.

(4) Produce unique data files and reports developed for use only at the battalion and/or extension centers.

(5) Process Electronic Forms (DOD, DA, TRADOC, etc.).

c. Use of Non-DOD computer networks is prohibited for transmission of cadet data containing bank account information, name or social security number (SSN). To ensure cadet confidentiality, the TC data (excluding reports, see 4-2d below) originating from the CCIMS will be accomplished using modems (point-to-point communications) between remote users (battalions, brigades, etc.) and region HQ.

d. Non-DOD computer networks may be used for e-mail connection to the region host computer. Care must be taken when attaching documents, such as CCIMS reports, to ensure

conformity wit para. 4-2c above.

e. Using University-Owned Computers. Connecting the CCIMS Computer to a university computer system is **NOT AUTHORIZED** except as follows:

(1) Battalions and extension centers will **NOT** allow any university computer to "dial-in" to the CCIMS Computer.

(2) Battalions or extension centers may receive data on floppy disk.

(3) Battalions and extension centers may connect to university-owned networks for the purposes of publishing and maintaining World Wide Web (WWW) Home Pages on university servers.

a. Battalion Home Pages' content should be limited to battalion-specific and campus-specific information, such as course schedules, campus features, schedules of upcoming events, and listings of cadre with contact names, telephone numbers, and e-mail addresses. It may also include a special list of cadets with e-mail addresses, to permit computer literate prospects to communicate with like-minded cadets.

b. Development and maintenance of Home Pages must be in accordance wit policies and guidelines established by HQ, Cadet Command and region HQ.

c. The PMS is ultimately responsible for the Battalion's Home Page. He or she should complete, sign, and submit the disclaimer/checklist to the region HQ.

(4) Battalions or extension centers may "dial in" to their university computer system for the purpose of queries and data transfer.

(5) Battalions and extension centers may directly connect university-owned PCs to their PCs provided that they are completely controlled and used ONLY by battalion or extension center personnel, and are not connected to another university computer system.

f. Battalions and extension centers must be careful about sharing data with their university because of Privacy Act considerations. Paper printouts may be shared provided they are properly marked "For Official Use Only," and in accordance with security and Privacy Act regulations. The Professor of Military Science (PMS) **WILL** sign a memorandum certifying that these safeguards have been taken. The signed memo will be attached to the first page of any printout or report.

g. If in doubt about sharing data and documents, CONSULT the region ADP security officer for guidance.

Chapter 5, Automated Information Systems (AIS) Accreditation TOC

5-1. Accreditation Overview

a. This policy includes the security accreditation of Army AIS and networks, which includes all HQ, U.S. Army Cadet Command, region HQ, brigades, battalions, extension centers, goldminers, and nurse units. All AIS computers will be accredited (**AR 380-19**, para. 3-1).

b. A designed accreditation authority (DAA) will be identified for all AIS within Cadet Command. Region HQ will function as DAA for the brigades, battalions, extension centers, goldminers, and nurse units within its command.

c. The DAA within the HQ, Cadet Command will be included in TRADOC's DOIM's accreditation plan.

5-2. Types of Accreditation

a. Generic accreditation is used for computer processing of unclassified, sensitive information (US-1 and US-2) fielded to multiple AIS users in lieu of separate accreditation for each computer. (Cadet Command processes US-2 type data.) Generic accreditation contains:

(1) Local Information Systems Security Officers Appointment Order.

(2) Local Security Standing Operating Procedures (SOPs).

(3) Facility Security Profile (FSP).

(4) Copy of signed authorization memo for each accredited US-1 and US-2 computer maintained in files.

b. Operational accreditation is applicable to all AIS that have not been accredited by a generic accreditation. Operational accreditation may also be required for AIS covered by a generic accreditation if AIS is operating within the security bounds of the generic accreditation

5-3. Accreditation Security Plan. Develop a security plan (see **AR 380-19**, Appendix C for format) and refine throughout the accreditation process.

Chapter 6, Security

TOC

6-1. Security

a. Security of automated information is essential to the efficient and effective management of Cadet Command. Data integrity (accuracy, completeness, and timeliness) is a must for sound decision making.

b. All security measures will meet the physical and fire security requirements of the host university or installation for its own automated seats.

c. All security procedures will conform to **AR 380-19,** Information Security and U.S.Title 18 concerning software policy.

d. An Information Systems Security Officer (ISSO) will be appointed by the PMS. The ISSO will prepare accreditation documents for each PC or network that is signed by the PMS and provide ADP security briefings and training.

e. Prepare a "Report of Survey" for each lost and stolen piece of hand receipted hardware and software.

f. Security of automated services comprises five separate areas: hardware, software, data files, environment, and personnel..

6-2. Hardware

a. Hardware refers to the physical elements that comprise a computer system, such as the Central Processing Unit (CPU), Compact Disk Read Only Memory (CD ROM), tape drives, modems, printers, and monitors. The protection of Government equipment is the responsibility of each individual who uses the equipment.

b. Some of the most common factors affecting hardware security are theft and damage. In order to reduce these risks and other security threats, the following procedures will be followed:

(1) All hardware will be kept in a locked room or a secured area. Only Cadre members will have unsupervised access to the keys.

(2) All computer equipment will be protected by an authorized power protector for the power and telephone lines.

(3) Magnetic media -- CD ROMs, tapes, diskettes, and cassettes -- must be protected to the same degree as the data they contain. All diskettes will be labeled with the contents and date.

(4) Diskettes must be protected from smoke, dust, drinks, food, and magnetic devices such as telephones and electrical motors.

(5) An active terminal must never be left unattended. Always log out or lock the terminal before leaving it.

(6) During electrical storms and other adverse weather conditions, the computers must be turned off and the equipment unplugged from the power source and telephones. If flooding is a possibility, equipment must be moved to higher facilities to eliminate water damage.

(7) Computers will be powered down at the end of the workday, unless data transfers are to be processed overnight.

6-3. Software

a. Software refers to the set of instructions placed into a computer's memory that tells the computer what to do.

b. Software may be obtained from a variety of sources -- Government purchase, public and commercial purchase, privately-owned, and shareware.

c. Protection of software is the responsibility of each user of the software. Software integrity can be maintained by preventing deliberate and unauthorized manipulation of software.

d. Two of the greatest hazards to software security are piracy and viruses. The following procedures will lessen security risks:

(1) government purchased software is regulated by its purchase license. This license allows

the user to "**USE, NOT OWN**" the software and its related documentation.

(2) It is a felony to copy software onto the hard drive of computers without written permission from the licensee. The user will NOT copy, reproduce, merge, modify, or transfer all or any portion of the software without written permission.

(3) Before **ANY** software is loaded on the Government computer, it must be checked with the Government issued "virus detection software." The **ISSO** will ensure that virus protection is used.

(4) Government licensed software will not be installed on privately-owned computers for off-site processing. Individuals taking official unclassified work home must use Government-owned equipment which has been authorized for processing off-site.

(5) Document all software, including the type of security required.

(6) When creating new software or modifying existing software, **DO NOT** use software in the production mode until it has been processed with test data and results have been validated.

(7) All operating systems, applications, off-the-shelf software, and back-up diskettes will be properly stored and "write protected" to prevent unapproved modifications and access by unauthorized users.

6-4. Data Files

a. Data security is the easiest and most often neglected of the security areas.

b. The following procedures will help to maintain data integrity:

(1) If you suspect someone has tampered with your files or data, report it to your local ISSO. The unit ISSO will report incidents to the Region ISSO, who will report it to the HQ, Cadet Command ISSO.

(2) Store data on diskettes with the "Write Protected" tab set.

(3) Restrict access to your data through the use of approved "User IDs." Only authorized personnel should have data files or information concerning cadets.

(4) Back up data and office automation files. It is imperative that schools back up their telecommunication files before telecommunicating with the region. Hosts and extension centers must compare their file transfer reports to the files received from the region to ensure that all data has been processed. Battalions are to restore any data files not processed by the region to their system for telecommunication.

6-5. Environment

a. Environmental security deals with the physical areas housing the ADP equipment. Some of the most common factors affecting environmental security are damage while moving, fluid spillage, fire, floods, and theft.

b. In order to reduce the risks of these and other threats, the following procedures will be adhered to:

(1) The main computer room and/or area will be locked when not occupied by authorized personnel. Key control and other access control will be available to a **LIMITED** number of personnel appointed by the PMS.

(2) Computers should be elevated above floor level and away from windows and doors to minimize damage from floods.

(3) Notify the Cadet Command Help Center before moving computers. They will provide detailed instructions for the move. Before beginning the move, bring the system down using your regular procedures. When the move has been completed, bring the computer up using your regular procedures.

(4) Preparation for adverse weather operations will include procedures listed in the Installation Adverse Weather Operations Plan (OPLAN). Battalions and extension centers will also follow University procedures.

6-6. Personnel

a. Efficient and dedicated personnel are the key to successful security measures.

b. The following procedures will aid in maintaining personnel security:

(1) A TASO will be appointed for systems with remote terminals communicating with a central computer.

(2) Passwords at all organizational levels will be changed frequently, not be shared, or compromised. Passwords will be changed at least annually and upon termination of any employee with access to CCIMS passwords.

Chapter 7, Accountability TOC

7-1. Hardware

a. Establish control and audit procedures through the Property Book Accountability and Audit Trails to ensure proper AIS use.

b. All "on-hand computers" (Desk Top and Personal Computers) acquired either through purchase (using Government Funds), lateral transfer, or DARIC will be accounted for on the unit's property book. Cite CTA 50-999 as applicable authority in the appropriate block on the property book page.

c. Donated automation equipment or equipment obtained from the school is not Army property and will not be picked up on the property book.

7-2. Software

All software purchased and distributed after the effective date of this regulation will be on a hand receipt, and will appear on the accreditation document for each PC. If the software is lost or stolen, a "Report of Survey" will be completed.

Chapter 8, Maintenance and Repair

TOC

8-1. Procedures and Policies

a. Headquarters, Cadet Command, region HQ, battalions, and extension centers will follow procedures and policies established by HQ, IMO, for maintenance and repair of CCIMS.

b. Battalions and extension centers will back up PCs on a regular basis and maintain these backups, as well as original copies of the software, in a secure place.

c. Battalions and extension centers are instructed to never disable the virus protection software or make hardware alterations (i.e., swapping out hard drives) unless specifically directed to do so by the Call Screening Center.

8-2. Maintenance and Repair

a. Maintenance and repair of the CCIMS PCs, printers, tape drives, and modems are the responsibility of the contractor who operates the Cadet Command "ROTC Call Screening Center." The toll-free number for the Call Screening Center is **1-800-750-ROTC (7682)**.

b. When placing a call to the ROTC Call Screening Center, please have available your school's **FICE Code** and an accurate description of the problem.

c. When a call results in the determination of a hardware problem, the following procedures must be followed:

(1) A replacement PC, along with instructions, will be shipped within 2 working days.

(2) Upon receipt of the replacement PC, the battalion/extension center will complete and return the PC Maintenance Survey Form included with the PC shipped from the Call Screening Center. The malfunctioning PC and **KEYS TO THE COMPUTER CASE** will be returned in the same shipping carton to the Call Screening Center.

(3) The battalion/extension center **WILL NOT REMOVE** any standard item of issue (i.e., memory chips, disk drives, tape drives, etc.).

(4) The battalion/extension center will, however, **remove** any item which was **non-standard** issue (i.e., CD ROM drives to include internal board). If a non-standard issue item is returned, the Call Screening Center is not contractually bound to pay return postage, and the item will be turned over to HQ, Cadet Command, Fort Monroe, VA. It will then become the battalion/extension center's responsibility to make arrangements for the return of said device at their expense.

(5) Neither the Call Screening Center nor HQ, Cadet Command, will be responsible for any missing parts.

Chapter 9, Training

9-1. Objective. The objective of battalion and extension center training is to ensure that the computer user will be able to properly perform all tasks associated with mission accomplishment through the use of automation.

9-2. Program of Instruction

a. Initial training for all personnel on the use of Government computers will be based on the Program of Instruction (POI) presented at the School of Cadet Command (SOCC) and regional locations by trained personnel.

b. Other training will be planned and executed by the IMO at HQ, Cadet Command, and region HQ.

Appendix A

AR 25-1
The Army Information Resources Management Program

AR 380-19
Information Systems Security

JOHN T. D. CASEY
Major General, U.S. Army
Commanding

OFFICIAL:

RODNEY A. PHILLIPS
Colonel, GS, U.S. Army
Chief of Staff

DISTRIBUTION: